IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

ST. ISIDORE RESEARCH, LLC, **Plaintiff,** **v.** **ALLY FINANCIAL INC., and ALLY BANK,** **Defendants.**	**Civil Action No. 2:15-cv-01549** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement arising under the Patent Laws of the United States of America, 35 U.S.C. § 1 *et seq*. in which Plaintiff St. Isidore Research, LLC ("St. Isidore" or "Plaintiff") makes the following allegations against Defendants Ally Financial Inc., and Ally Bank, (collectively, "Ally" or "Defendants").

BACKGROUND

1. Alexander W. Evans is an inventor and entrepreneur who, in the early 2000's invented systems and methods in the field of personal and financial data security. Mr. Evans recognized the proliferation of mobile devices could be used to verify, authenticate, and provide notification of commercial and financial transactions.

2. Mr. Evans has served as a senior executive in Fortune 500, public, and privately held companies in the IT and telecommunications sectors. He holds a Masters of Business Administration from Harvard University and a Bachelors of Science in Electrical Engineering from Yale University. Mr. Evans is the owner and Chief Executive Officer of St. Isidore.

3. Mr. Evans worked to develop novel technical solutions to protect and authenticate data transactions. Mr. Evans' inventions led to the filing of the patent applications resulting in U.S. Patent No. 7,904,360 ("the '360 patent") and U.S. Patent No. 8,589,271 ("the '271 patent") (collectively, "the St. Isidore patents").

4. Plano, Texas based St. Isidore is committed to advancing the current state of technology in the field of transaction security. In addition to the ongoing efforts of Mr. Evans, St. Isidore employs an Allen, Texas resident with a Ph.D. in Electrical Engineering from the University of Oklahoma as its Vice President of Technology.

5. Mr. Evans is the owner of St. Isidore.

6. Companies including Defendants have adopted the inventions disclosed in the St. Isidore patents.

7. The St. Isidore patents have been cited in patents and patent applications filed by companies including: Apple, Alcatel Lucent, JP Morgan Chase, AT&T, Nortel, IBM, American Express, Visa, and First Data Corporation.

U.S. PATENT NO. 7,904,360

8. St. Isidore is the owner by assignment of the ’360 patent. The ’360 patent is entitled “System and Method for Verification, Authentication, and Notification of a Transaction.” The ’360 patent issued on March 8, 2011, based on a patent application filed on January 30, 2003. A true and correct copy of the ’360 patent is attached hereto as Exhibit A. The ’360 patent claims specific methods and systems for authenticating a device for use in accessing information related to an associated account.

9. The claims in the ’360 patent (“’360 claims”) are directed at a technical solution to a problem unique to computer networks – the authentication of a transaction conducted on an electronic device using at least two communication links (*e.g.*, SMS and HTTP).

10. Processing and authenticating a transaction conducted on an electronic device presented new and unique issues over the state of the art at the time. “[T]here is a prevailing public perception that electronic purchasing environments (for example, virtual storefronts or Internet auctions) are inherently insecure in regard to the transmission and/or storage of private information.” ’360 patent 1:66-2:3.

11. Although the systems and methods taught in the ’360 claims have been widely adopted by leading businesses today, at the time of invention, the technologies taught in the ’360

claims were an innovative and "inventive system . . . providing [] users with a programmable message content and formatting mechanism that need not be maintained in or supplied to the inventive system, but may instead be incorporated dynamically, by reference, at the time the transaction is processed." '360 patent 18:41-47.

12. Further the '360 claims improve upon the functioning of a computer system by allowing the more efficient and less resource intensive processing of transactions. "Note that in a large-scale embodiment, the inventive system is likely to process a large volume of Transaction Messages and Transaction Objects concurrently, via multithreaded processing and load-balancing among multiple processors and subsystems, and its design should not be construed as requiring serial processing of Transaction Messages and Transaction Objects." '360 patent 22:23-29.

13. One or more of the '360 claims relate to a computer-implemented method and/or system to process, transform and authenticate a transaction in a particular manner – by inserting information into a transaction and using code to authenticate a device to perform a transaction, this insertion enables a particular device to be authenticated for the purposes of processing a transaction.

14. The '360 claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to the a narrow set of methods and systems for "verifying" and "authenticati[ng]" transactions over a computer "network."

15. The '360 claims are not directed at the broad concept/idea of "authenticating" or "verifying" transactions. Instead, the claims are directed at very particular, narrow methods and systems for "authenticating" and "verifying" transactions on electronic devices using technologies unique to the internet age. The inventive concept in the '360 claims is a technological one rather than an entrepreneurial one. The use of two or more communications links to verify a transaction on an electronic device is a specific solution to the technological problem of verifying and authenticating transactions in the internet age.

16. The ’360 claims are directed toward a solution rooted in computer technology and use technology unique to computers and networks to overcome a problem specifically arising in the realm of verifying transactions on computer networks. For example, the ’360 claims are directed toward “verifying” and “authenticating” transactions over a network (*e.g.*, the Internet) using electronic devices which are specially configured to yield a desired result—a result that overrides the routine and conventional sequence of events ordinarily triggered by merely attempting to authenticate a transaction by having a user enter a user name and password.

17. The use of two or more communications links to verify and authenticate a transaction on an electronic device was not a longstanding or fundamental economic practice at the time of invention of the ’360 patent. The use of two separate communications links to determine the authenticity of a transaction on an electronic device was not at the time of the invention a fundamental principle in ubiquitous use on the Internet or computers in general.

18. The ’360 claims are not directed at a method for organizing human activity as the ’360 claims teach specific systems and methods for authenticating and verifying transactions on electronic devices using two or more communications links.

19. The ’360 claims are not directed at a mathematical relationship or formula as the ’360 claims teach specific systems and methods for authenticating and verifying transactions on electronic devices using two or more communications links.

20. The invention claimed in the ’360 patent goes beyond manipulating, reorganizing, or collecting data by actually adding information associated with a transaction and receiving that information via a first communications link thereby fundamentally altering information associated with the transaction.

21. One or more of the ’360 claims requires “transforming” data associated with a verification request by adding a unique verification identifier. The ’360 claims further recite a particular manner of transforming a verification request by requiring the addition of a unique verification identifier. Therefore, the claimed features in the ’360 claims fundamentally alter data associated with a verification request and go beyond the mere collection, organization,

manipulation, or reorganization of data.

22. One or more of the ’360 claims require a specific configuration of electronic devices and the use of communication protocols to verify and authenticate transactions and are meaningful limitations that tie the claimed methods and systems to specific machines.

23. One or more of the ’360 claims go beyond manipulating, reorganizing, or collecting data by actually adding new information to a verification request, thereby fundamentally altering a verification request.

24. The ’360 claims not only recite a process for verifying transactions, the claims involve a protocol for making the computer implemented system itself more secure. “It is also an object of the invention to allow said communications to occur over a plurality of communications media and/or communications links, to increase the likelihood of successful and secure communication with and/or to said one or more parties.” ’360 patent 8:48-52.

25. The ’360 claims cannot be performed by a human, in the mind, or by pen and paper. The claims as a whole are directed to verifying and authenticating a transaction on an electronic device using a first communications link, transmitting via a second communications link a verification request, identifying a party associated with a transaction using a computer, and processing the transaction initiated over a first communications link. These limitations require two communications links (*e.g.*, SMS messaging capability and HTTP communications), a computer system configured to process a transaction, a computer system configured to identify a party associated with a transaction, and a computer system capable of transmitting over two different communications links – all elements that cannot be done by a human, in one’s mind, or by paper and pencil.

26. One or more of the ’360 claims require an external data storage unit containing information to identify a party, a database connected to the computer system that contains data for matching the unique verification identifier, a computer system capable of formatting a communication into an XML document and/or XLS stylesheet, a computer system capable of simultaneously communicating over two communications links, and/or the use of middleware

having a message queuing capability. These claim limitations cannot be performed in the human mind or by pen and paper.

27. The use of a unique verification identifier sent over a communications link is not a conventional activity that humans engaged in before computers.

28. Authenticating a transaction using two or more different communications links where the communications links communicate via public switched telephone network (PSTN), wireless telephony, text messaging, short message service (SMS), internet, telex, paging service, email, an EDI/EDIFACT/EDI-INT network, an IBM System Network Architecture/Remote Job Entry (SNA/RJE), SMTP, HTML, XHTML, and/or XML, is not something that is a conventional activity that humans are capable of performing mentally or by pen and paper.

29. One or more of the '360 claims require a fixed step-by-step procedure using two different communications links for accomplishing the verification of a transaction.

30. The prior art cited on the face of the '360 patent further show that the invention disclosed in the '360 claims is not a patent ineligible abstract idea. The invention taught in the '360 claims is narrower than at least some of the cited prior art, and therefore, is not an abstract idea. For example, U.S. Pat. No. 6,182,894 to Hackett describes systems and methods to use CVV2/CVC2/CID values, in lieu of PIN codes, to verify that a consumer engaged in a point-of-sale (POS) transaction. The '360 claims require the use of two or more different communications links to verify a transaction. This requirement is absent in the Hackett patent and thus the '360 claims are directed toward significantly more than an abstract idea and the '360 claims do not preempt the field of transaction verification.

31. The claimed invention in the '360 claims is rooted in computer technology and overcame a problem specifically arising in the realm of computer networks. At the time of invention, limitations in the prior art that the '360 patent was directed to solving included:

- Identity theft: "particularly for e-commerce transactions, [transmitting personal information] is vulnerable to theft via hacking of the merchant's systems or interception of the merchant's communications to the payment-processing bank or

applicable credit card processing network." '360 patent 5:32-36.

- Verifying an electronic transaction request: "there is a prevailing public perception that electronic purchasing environments (for example, virtual storefronts or Internet auctions) are inherently insecure in regard to the transmission and/or storage of private information." '360 patent 1:66-2:3.
- Verifying a transaction on a mobile device: "The invention relates to fraud prevention and fraud 'early warning' notifications, in particular remote and/or electronic transactions such as 'e-commerce' and 'm-commerce.'" '360 patent 1:13-16.

32. The '360 claims require the use of a computer system. The use of a computer system plays a significant part in permitting the claimed methods to be performed. For example, the use of two communications links to verify a transaction is integral to the success of the transaction and can only be performed using a computer system. The use of a computer system communicating over two communications links does not only allow the verification and authentication of a transaction to be performed more quickly, it is integral to accomplish the verification and authentication of a transaction in a secure manner.

33. The '360 claims do not preempt a field or preclude the use of other effective verification and authentication techniques. The '360 claims include inventive elements such as the use of two different communications links to verify and authenticate a transaction and transmitting a verification request over a second communications link. The elements in the '360 claims greatly limit the breadth of the '360 claims. These limitations are not necessary or obvious tools for achieving transaction verification and authentication, and they ensure that the claims do not preempt other techniques for transaction verification and authentication. Other techniques for transaction verification and authentication that would not be included in the scope of the '360 claims include, but is not limited to, the prior art discussed the patent:

- U.S. Pat. No. 6,182,894 to Hackett describes systems and methods to use CVV2/CVC2/CID values, in lieu of PIN codes.
- U.S. Pat. No. 5,727,163 to Bezos describes a system and method for concluding a transaction by telephone that was initiated over the Internet.
- U.S. Pat. No. 6,324,526 to D'Agostino describes a system and method for providing a transaction code, supplied case by case by the purchaser's financial institution, in

lieu of a credit card number for a purchase transaction.

- U.S. Pat.No. 6,270,011to Gottfried describes a system and method for coupling a fingerprint recognition device to a credit card scanner.
- U.S. Pat. No. 6,341,724 to Campisano describes a system and method for using the telephone number of a credit card owner, plus a PIN code, as an alias for the actual card number in a credit card transaction.
- U.S. Pat. No. 6,023,682 to Checchio describes a system and method for communicating a credit card number to a payment-authorizing computer system from a point-of-sale credit card terminal, using encryption.
- U.S. Pat. No. 6,088,683 to Jalili describes a method for customers to order goods from merchants on one network, such as the Internet, and then complete the purchase via a second network, such as the telephone network, using "Caller ID" service or a call-back.

34. The '360 claims do not preempt transaction verification and authentication as numerous technologies are available. These technologies may include, but are not limited to, the following: (1) the use of hardware tokens, (2) encryption with a strong password, (3) biometrics, and (4) image based authentication.

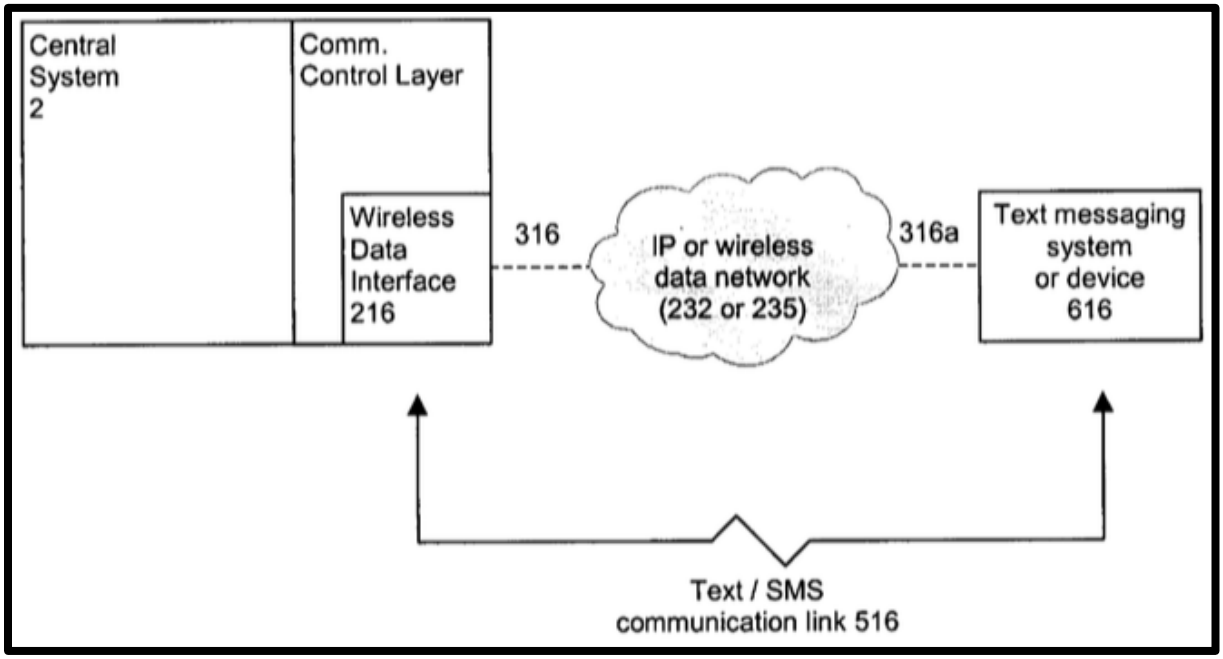
35. The '360 claims are directed toward solving the problem of verifying and authenticating an e-commerce or m-commerce transaction where the ephemeral nature of an internet "location" and the near-instantaneous ability to make a transaction request by a non-merchant is made possible by standard internet communication protocols. This technical problem does not exist in traditional "brick and mortar" stores where customers are at the store when requesting to conduct a transaction.

36. The '360 claims not only recite a process for verifying transaction information, the claims involve a protocol for making the computer system itself more secure. The invention disclosed in the '360 claims have a concrete effect in verifying, authenticating, and processing electronic transactions. The claims are directed to solving a technological problem of verifying e-commerce and m-commerce transactions. The prior art discussed in the '360 patent shows that the '360 claims are directed at solving this problem using unconventional and novel techniques.

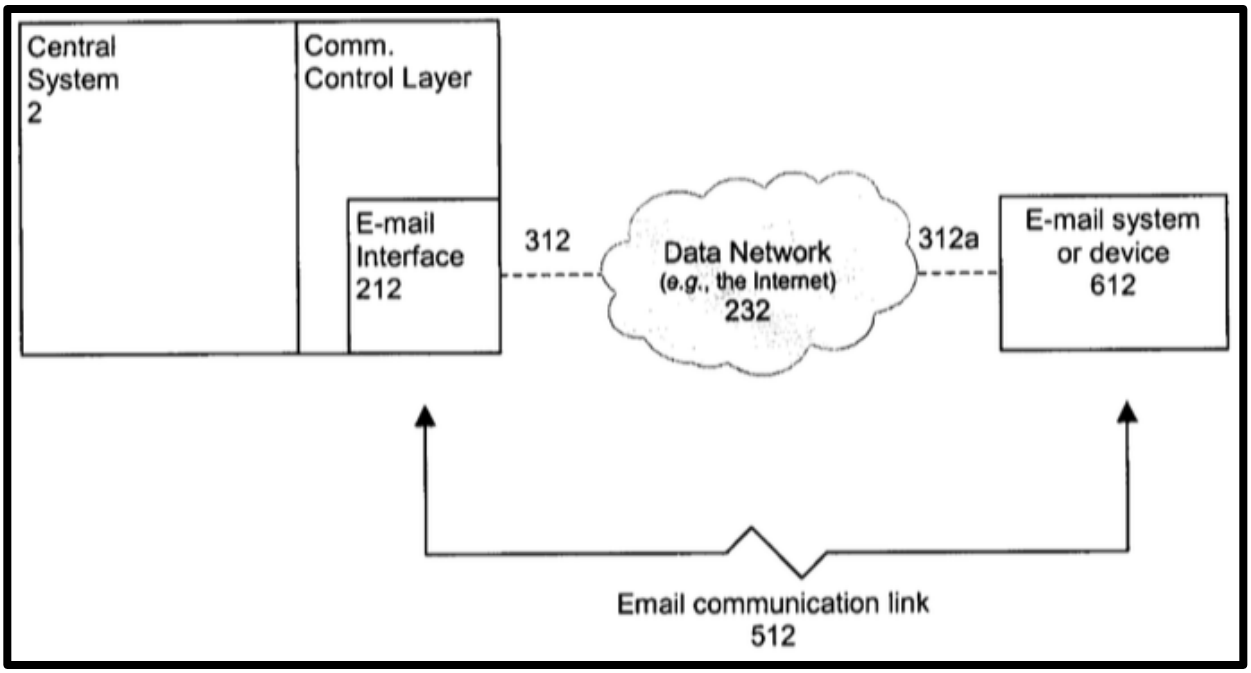
37. The use of party-specific, device-specific, and/or user-predefined parameters to authenticate a transaction confers benefits on a computer system. "The use of these party- and

device-specific, user-predefined parameters to guide the inventive system in its interaction attempts with a party provides the invention with the advantage of a high degree of flexibility and effectiveness in getting through to a party with a minimum of difficulty." '360 Patent 25:33-38.

38. The '360 claims require steps that are not conventional or routine. The use of two different communications links to verify a transaction was not ubiquitous at the time of invention. Further, elements in the dependent claims of the '360 patent require additional steps that are not conventional or routine.



'360 Patent Fig. 16 (describing passing of SMS verification information to a device).



'360 Patent Fig. 12 (describing passing of email verification information to a device).

U.S. PATENT NO. 8,589,271

39. St. Isidore is the owner by assignment of the '271 patent. The '271 patent is entitled "System and Method for Verification, Authentication, and Notification of Transactions." The '271 patent issued on November 19, 2013, based on a patent application filed on February 3, 2012. A true and correct copy of the '271 patent is attached hereto as Exhibit B. The '271 patent claims specific methods and systems for authenticating a device for use in accessing information related to an associated account.

40. The claims in the '271 patent ("'271 claims") are directed at a technical solution to a problem unique to computer networks – the authentication of an electronic device to be associated with an account using at least two devices (*e.g.*, computer and mobile devices).

41. Authenticating an electronic device presented new and unique issues over the state of the art at the time. "[T]here is a prevailing public perception that electronic purchasing environments (for example, virtual storefronts or Internet auctions) are inherently insecure in regard to the transmission and/or storage of private information." '271 patent 2:4-8.

42. Although the systems and methods taught in the '271 claims have been widely

adopted by leading businesses today, at the time of invention, the technologies taught in the '271 claims were an innovative and "inventive system . . . providing [] users with a programmable message content and formatting mechanism that need not be maintained in or supplied to the inventive system, but may instead be incorporated dynamically, by reference, at the time the transaction is processed." '271 patent at 25:5-11.

43. Further the '271 claims improve upon the functioning of a computer system by allowing the more efficient and less resource intensive processing of transactions. "Note that in a large-scale embodiment, the inventive system is likely to process a large volume of Transaction Messages and Transaction Objects concurrently, via multithreaded processing and load-balancing among multiple processors and subsystems, and its design should not be construed as requiring serial processing of Transaction Messages and Transaction Objects." '271 patent 29:16-23.

44. One or more of the '271 claims relate to a computer-implemented method and/or system to authenticate a device to be associated with an account in a particular manner – by receiving an account access request from a first device and using a verification message via a second device to authenticate the first device, enables a particular device to be authenticated for the purposes of being associated with an account.

45. The '271 claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to the a narrow set of methods and systems for "verifying" and "authenticati[ng]" devices over a computer "network."

46. The '271 claims are not directed at the broad concept/idea of "authenticating" or "verifying" devices. Instead, the claims are directed at very particular, narrow methods and systems for "authenticating" and "verifying" electronic devices using technologies unique to the internet age. The inventive concept in the '271 claims is a technological one rather than an entrepreneurial one. The use of two or more devices to authenticate a device to be associated with an account is a specific solution to the technological problem of verifying and

authenticating devices in the internet age.

47. The ’271 claims are directed toward a solution rooted in computer technology and use technology unique to computers and networks to overcome a problem specifically arising in the realm of verifying devices on networks. For example, the ’271 claims are directed toward “verifying” and “authenticating” devices over networks (*e.g.*, the Internet) using at least two electronic devices which are specially configured to yield a desired result—a result that overrides the routine and conventional sequence of events ordinarily triggered by merely attempting to authenticate a device by having a user enter a user name and password.

48. The use of two or more devices to verify and authenticate an electronic device was not a longstanding or fundamental economic practice at the time of invention of the ’271 patent. The use of two separate devices to determine the authenticity of an electronic device was not at the time of the invention a fundamental principle in ubiquitous use on the Internet or computers in general.

49. The ’271 claims are not directed at a method for organizing human activity as the ’271 claims teach specific systems and methods for authenticating and verifying an electronic device to be associated with an account using two or more devices.

50. The ’271 claims are not directed at a mathematical relationship or formula as the ’271 claims teach specific systems and methods for authenticating and verifying an electronic device to be associated with an account using two or more devices.

51. The invention claimed in the ’271 patent goes beyond manipulating, reorganizing, or collecting data by actually adding information associated with an account and having a device receive that information via a network thereby fundamentally altering information associated with the account.

52. One or more of the ’271 claims requires “transforming” data associated with a verification request by adding a unique verification message. The ’271 claims further recite a particular manner of transforming a verification request by requiring the addition of a unique verification message. Therefore, the claimed features in the ’271 claims fundamentally alter data

associated with a verification request and go beyond the mere collection, organization, manipulation, or reorganization of data.

53. One or more of the ’271 claims require a specific configuration of electronic devices and the use of communication protocols to verify and authenticate devices and are meaningful limitations that tie the claimed methods and systems to specific machines.

54. One or more of the ’271 claims go beyond manipulating, reorganizing, or collecting data by actually adding new information to a verification request, thereby fundamentally altering a verification request.

55. The ’271 claims not only recite a process for authenticating devices to be associated with an account, the claims involve a protocol for making the computer implemented system itself more secure. “It is also an object of the invention to allow said communications to occur over a plurality of communications media and/or communications links, to increase the likelihood of successful and secure communication with and/or to said one or more parties.” ’271 patent 8:52-56.

56. The ’271 claims cannot be performed by a human, in the mind, or by pen and paper. The claims as a whole are directed to verifying and authenticating an electronic device to be associated with an account by receiving an account access request from a first device, transmitting to a second device a verification message associated with account access request, receiving a response related to the verification message, and verify the authenticity of the account access request based on the response, so that one or more subsequent requests to access the account from the first device is granted without communicating with the second device. These limitations require two devices (*e.g.*, mobile phone and computer), a computer system configured to process access requests, and networks configured to transmit information to two different devices – all elements that cannot be done by a human, in one’s mind, or by paper and pencil.

57. One or more of the ’271 claims require an database for storing authentication information, and/or a database connected to the computer system that contains data for matching

the unique verification message to a device. These claim limitations cannot be performed in the human mind or by pen and paper.

58. The use of a unique verification message being transmitted to a different device is not a conventional activity that humans engaged in before computers.

59. Authenticating a device to be associated with an account using two or more different devices via networks comprising at least one of a public switched telephone network (PSTN), wireless telephony, text messaging, short message service (SMS), internet, telex, paging service, email, an EDI/EDIFACT/EDI-INT network, an IBM System Network Architecture/Remote Job Entry (SNA/RJE), SMTP, HTML, XHTML, and/or XML, is not something that is a conventional activity that humans are capable of performing mentally or by pen and paper.

60. One or more of the ’271 claims require a fixed step-by-step procedure using two different devices for accomplishing the authentication of a device to be associated with an account.

61. The prior art cited on the face of the ’271 patent further show that the invention disclosed in the ’271 claims is not a patent ineligible abstract idea. The invention taught in the ’271 claims is narrower than at least some of the cited prior art, and therefore, is not an abstract idea. For example, U.S. Pat. No. 6,182,894 to Hackett describes systems and methods to use CVV2/CVC2/CID values, in lieu of PIN codes, to verify that a consumer engaged in a point-of-sale (POS) transaction. The ’271 claims require the use of two or more devices to authenticate a device to be associated with an account. This requirement is absent in the Hackett patent and thus the ’271 claims are directed toward significantly more than an abstract idea and the ’271 claims do not preempt the field of device authentication.

62. The claimed invention in the ’271 claims is rooted in computer technology and overcame a problem specifically arising in the realm of computer networks. At the time of invention, limitations in the prior art that the ’271 patent was directed to solving included:

- Identity theft: "particularly for e-commerce transactions, [transmitting personal information] is vulnerable to theft via hacking of the merchant's systems or interception of the merchant's communications to the payment-processing bank or applicable credit card processing network." '271 patent 5:37-41.
- Verifying an electronic transaction request: "there is a prevailing public perception that electronic purchasing environments (for example, virtual storefronts or Internet auctions) are inherently insecure in regard to the transmission and/or storage of private information." '271 patent 2:4-8.
- Verifying a transaction on a mobile device: "The invention relates to fraud prevention and fraud 'early warning' notifications, in particular remote and/or electronic transactions such as 'e-commerce' and 'm-commerce.'" '271 patent 1:19-22.

63. The '271 claims require the use of a system. The use of a system plays a significant part in permitting the claimed methods to be performed. For example, the use of two devices to authenticate a device to be associated with an account is integral to the success of authenticating the device and can only be performed using a system. The use of a system communicating to two different devices does not only allow the verification and authentication of a device to be performed more quickly, it is integral to accomplish the verification and authentication of a device in a secure manner.

64. The '271 claims do not preempt a field or preclude the use of other effective verification and authentication techniques. The '271 claims include inventive elements such as the use of two different devices to verify and authenticate a device to be associated with an account and transmitting a verification message to a second device. The elements in the '271 claims greatly limit the breadth of the '271 claims. These limitations are not necessary or obvious tools for achieving device verification and authentication, and they ensure that the claims do not preempt other techniques for device verification and authentication. Other techniques for device verification and authentication that would not be included in the scope of the '271 claims include, but is not limited to, the prior art discussed the patent:

- U.S. Pat. No. 6,182,894 to Hackett describes systems and methods to use CVV2/CVC2/CID values, in lieu of PIN codes.
- U.S. Pat. No. 5,727,163 to Bezos describes a system and method for concluding a

transaction by telephone that was initiated over the Internet.

- U.S. Pat. No. 6,324,526 to D'Agostino describes a system and method for providing a transaction code, supplied case by case by the purchaser's financial institution, in lieu of a credit card number for a purchase transaction.
- U.S. Pat.No. 6,270,011to Gottfried describes a system and method for coupling a fingerprint recognition device to a credit card scanner.
- U.S. Pat. No. 6,341,724 to Campisano describes a system and method for using the telephone number of a credit card owner, plus a PIN code, as an alias for the actual card number in a credit card transaction.
- U.S. Pat. No. 6,023,682 to Checchio describes a system and method for communicating a credit card number to a payment-authorizing computer system from a point-of-sale credit card terminal, using encryption.
- U.S. Pat. No. 6,088,683 to Jalili describes a method for customers to order goods from merchants on one network, such as the Internet, and then complete the purchase via a second network, such as the telephone network, using "Caller ID" service or a call-back.

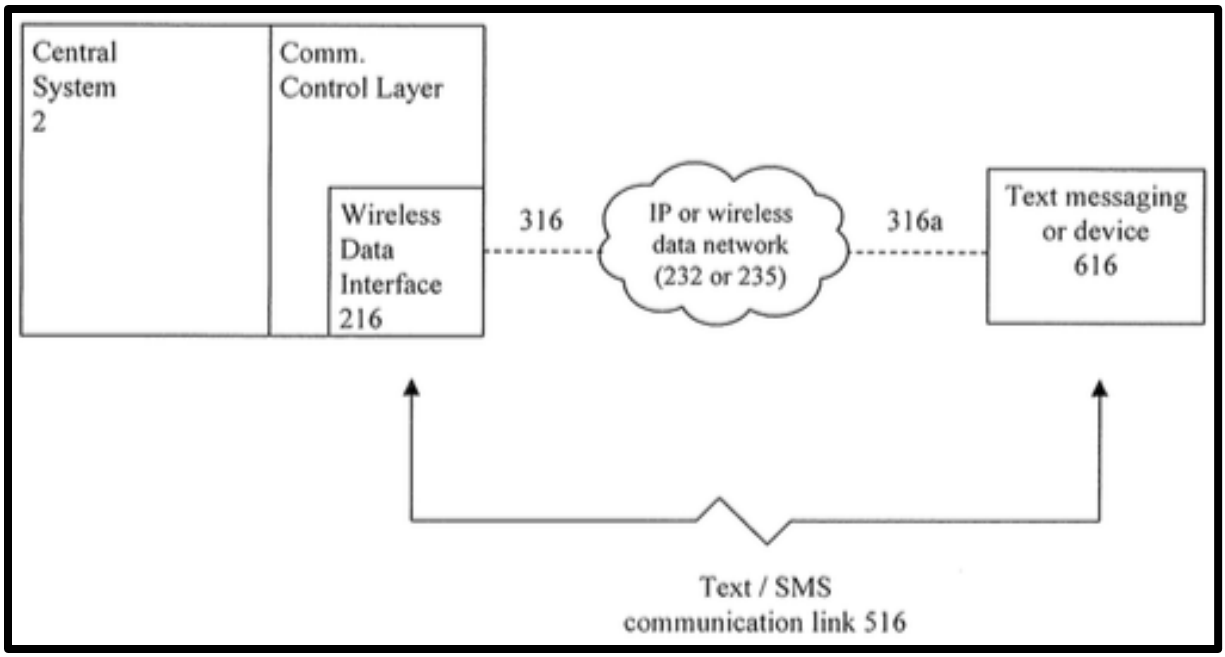
65. The '271 claims do not preempt device verification and authentication as numerous technologies are available. These technologies may include, but are not limited to, the following: (1) the use of hardware tokens, (2) encryption with a strong password, (3) biometrics, and (4) image based authentication.

66. The '271 claims are directed toward solving the problem of verifying and authenticating a device to be associated with an account where the ephemeral nature of a device or internet "location" and the near-instantaneous ability to access an account is made possible by standard internet communication protocols. This technical problem does not exist in traditional "brick and mortar" stores where customers are at the store when requesting to conduct a transaction.

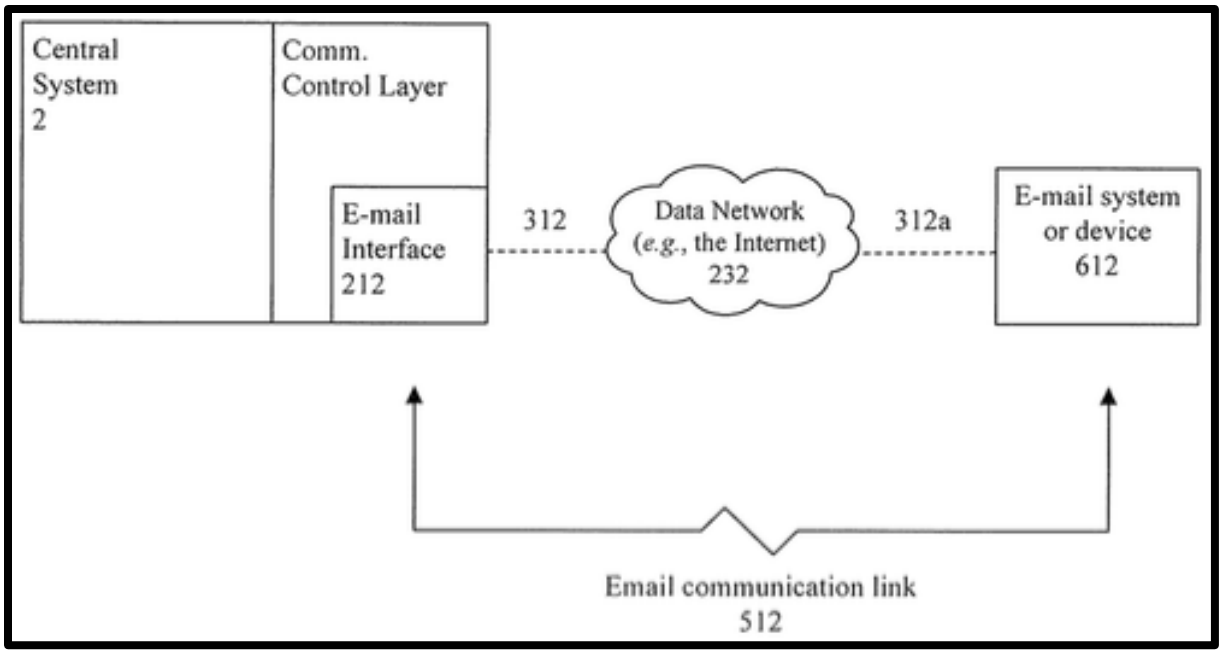
67. The '271 claims not only recite a process for authenticating devices, the claims involve a protocol for making the authenticating system itself more secure. The invention disclosed in the '271 claims have a concrete effect in verifying and authenticating devices. The claims are directed to solving a technological problem of verifying a device to be associated with an account. The prior art discussed in the '271 patent shows that the '271 claims are directed at solving this problem using unconventional and novel techniques.

68. The use of party-specific, device-specific, and/or user-predefined parameters to authenticate device confers benefits on a computer system. "The use of these party- and device-specific, user-predefined parameters to guide the inventive system in its interaction attempts with a party provides the invention with the advantage of a high degree of flexibility and effectiveness in getting through to a party with a minimum of difficulty." '271 Patent 32:65-33:3.

69. The '271 claims require steps that are not conventional or routine. The use of two different devices to authenticate a device to be associated with an account was not ubiquitous at the time of invention. Further, elements in the dependent claims of the '271 patent require additional steps that are not conventional or routine.



'271 Patent Fig. 9 (describing passing of SMS verification information to a device).



'271 Patent Fig. 5 (describing passing of email verification information to a device).

PARTIES

70. St. Isidore is a Texas limited liability company with a principal place of business at 903 E. 18th Street, Suite 121, Plano, Texas 75074.

71. On information and belief, Ally Financial Inc. is a Delaware corporation with its principal place of business at 200 Renaissance Center, Detroit, Michigan 48265-2000. On information and belief, Ally Financial Inc. is registered to do business in the State of Texas and it may be served with process by delivering a summons and a true and correct copy of this complaint to its registered agent for receipt of service of process, C T Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201-3136.

72. On information and belief, Ally Bank is a Utah corporation and an indirect wholly-owned subsidiary of Ally Financial Inc. with its principal place of business at 300 GM Renaissance Center MC 482-C14-C66, Detroit, Michigan 48265-00001. On information and belief, Ally Bank is registered to do business in the State of Texas and it may be served with process by delivering a summons and a true and correct copy of this complaint to its registered agent for receipt of service of process, C T Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201-3136.

JURISDICTION AND VENUE

73. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

74. This Court has personal jurisdiction over Defendants because, among other reasons, Defendants have established minimum contacts with the forum state of Texas. Defendants, directly and/or through third-party intermediaries, make, use, import, offer for sale, and/or sell products within the state of Texas, and particularly within the Eastern District of Texas. Thus, Defendants purposefully availed themselves of the benefits of doing business in the State of Texas and the exercise of jurisdiction over Defendants would not offend traditional notions of fair play and substantial justice. Specifically, Defendants own and operate numerous banking locations in the Eastern District of Texas.

75. Venue is proper in this District under 28 U.S.C. §§ 1391 (b)-(c) and 1400(b) because Defendants are subject to personal jurisdiction in this District, have transacted business in this district and have committed acts of patent infringement in this district.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 7,904,360

76. St. Isidore references and incorporates by reference paragraphs 1 through 75 of this Complaint.

77. Ally makes, uses, sells, and/or offers for sale in the United States products and/or services for authenticating and verifying transactions. On information and belief, at least some of Ally's transaction security products and/or services provide or support authenticating and verifying a transaction using two different communications links as described and claimed in the '360 patent.

78. Ally operates the Internet site https://www.ally.com/ ("Ally Site").

79. Ally has created and offers to its customers Ally Online Banking.

80. On information and belief, Ally Online Banking allows Ally to conduct banking

transactions involving mobile devices.

81. On information and belief, Ally Online Banking is "secure."

82. On information and belief, Ally Online Banking is available to anyone who has an Ally account.

83. On information and belief, Ally Online Banking uses a six-digit security code that is associated with the device of a banking customer.

84. On information and belief, it is advantageous for Ally Online Banking to be authenticated to conduct a banking transaction using the six-digit security code.

85. On information and belief, it is advantageous for Ally to be able to determine if a transaction and/or device is properly authenticated using the security code.

86. On information and belief, the six-digit security code used to authenticate a device for Ally is unique to each customer's device.

87. On information and belief, Ally Online Banking users "[i]f you already have an Ally Bank online account with a username and password, you can log in to allybank.com from your computer. . . [and can use a] Security Code in Online Banking [which is] a 6-digit code that you can ask us to send in a text message or email when you log in from a device we don't recognize."[1]

88. On information and belief, the six-digit security code is a "The code can only be used once, and expires 20 minutes after it's sent."[2]

89. On information and belief, for Ally Online Banking users, "[i]f you're on a personal computer that you use frequently it's a good idea to register it. If you're on a friend's computer or a computer used by the public you should not register it."[3]

90. On information and belief, Ally Online Banking allows users to (a) check your current Ally Bank account balance[s], (b) transfer funds between an Ally Bank Interest Checking

[1] http://www.ally.com/help/bank/login.html
[2] *Id.*
[3] *Id.*

Account, Money Market Account and Online Savings Account and non-Ally accounts, (c) see up to 18 months of account activity, (d) use Ally Email to communicate securely with Customer Care for any questions about accounts and transactions, (e) change your personal information, such as your street address, email, phone, password, secret question, and telephone Personal Identification Number (PIN), (f) search and find specific transactions, (g) use our free Bill Pay service to pay bills online, (h) place and/or remove stop payments, (i) request checks, deposit slips, and forms.[4]

91. On information and belief, for Ally Online Banking users, "[i]n Ally's online banking application you chose to have a security code sent to you via text message. This message will only be sent once for each send request."[5]

92. On information and belief, Ally "use[s] a layered security approach that includes . . . activat[ing] extra security measures like asking you a question that only you know the answer to or sending a security code to a device that you've registered. This is often called **2-step, 2-factor or multi-factor authentication**."[6]

93. On information and belief, "Many financial institutions like Ally have 2-step or 2-factor authentication built into their security solutions, but it's still smart to enable multi-factor verification on sites and devices where this feature is optional. Multi-factor authentication offers another layer of protection by asking for an extra piece of information in addition to your password, like a security code that's sent via text or a fingerprint ID. You can usually **enable 2-factor verification in your password and security settings**."[7]

94. On information and belief, Ally identifies the party associated with a transaction conducted on a device running the Ally Online Banking.

95. On information and belief, Ally receives via the Ally website information associated with a transaction request.

---

[4] http://www.ally.com/help/bank/login.html#regional=online-mobile-banking
[5] http://www.ally.com/messages/sms/index.html
[6] http://www.ally.com/security/
[7] https://www.ally.com/security/password-security-tips.html

96. On information and belief, Ally transmits a verification request to a customer to verify a transaction.

97. On information and belief, Ally determines the authenticity of a transaction based on the six-digit security code sent from a device running Ally Online Banking.

98. On information and belief, Ally authenticates a device running Ally Online Banking using two-factor authentication.

99. On information and belief, Ally electronically determines an identification of an authorized device, such as a mobile phone or computer associated with an account, based (in part) on the six-digit security code.

100. On information and belief, the Ally website transmits data over the Internet using at least the HTTP and/or HTTPS protocols.

101. On information and belief, devices running the Ally Online Banking transmit information over a mobile network.

102. On information and belief, the six-digit security code associated with a device running Ally Online Banking can be transmitted over a mobile network.

103. On information and belief, the six-digit security code is a user ID, PIN number, password, passcode, and/or user-defined party identifier.

104. On information and belief, Ally authenticates at least one party associated with a transaction by matching the six-digit security code with data stored in one or more databases.

105. On information and belief, the authentication of a device running Ally Online Banking is determined via a second communications link. This communications link could comprise a SMS text message from or a telephone call to Ally.

106. On information and belief, the communication of a message for authenticating a transaction comprises a message such as an email that utilizes middleware with queuing capability.

107. On information and belief, the authentication of a transaction is time sensitive such that a verification message must be received during a predetermined time period.

108. On information and belief, Ally has directly infringed and continues to infringe the '360 patent by, among other things, making, using, offering for sale, and/or selling transaction verification and authentication products and/or services. Such transaction security products and/or services include, by way of example and without limitation, use of Ally Online Banking system, which is covered by one or more claims of the '360 patent, including but not limited to claim 1.

109. By making, using, offering for sale, and/or selling transaction security products and/or services infringing the '360 patent, Ally has injured St. Isidore and is liable to St. Isidore for direct infringement of the '360 patent pursuant to 35 U.S.C. § 271(a).

110. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '360 patent.

111. As a result of Ally's infringement of the '360 patent, St. Isidore has suffered monetary damages in an amount adequate to compensate for Defendants' infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants, together with interest and costs as fixed by the Court, and St. Isidore will continue to suffer damages in the future unless Defendants' infringing activities are enjoined by this Court.

112. Unless a permanent injunction is issued enjoining Defendants and their agents, servants, employees, representatives, affiliates, and all others acting or in active concert therewith from infringing the '360 patent, St. Isidore will be greatly and irreparably harmed.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 8,589,271

113. St. Isidore references and incorporates by reference paragraphs 1 through 110 of this Complaint.

114. Ally makes, uses, sells, and/or offers for sale in the United States products and/or services for authenticating and verifying transactions. On information and belief, at least some of Ally's transaction security products and/or services provide or support authenticating and verifying a device to be associated with an account using two different devices as described and

claimed in the '271 patent.

115. Ally operates the Internet site https://www.ally.com/ ("Ally Site").

116. Ally has created and offers to its customers Ally Online Banking.

117. On information and belief, Ally Online Banking allows Ally to conduct banking transactions involving mobile devices.

118. On information and belief, Ally Online Banking is "secure."

119. On information and belief, Ally Online Banking is available to anyone who has an Ally account.

120. On information and belief, Ally Online Banking uses a six-digit security code that is associated with the device of a banking customer.

121. On information and belief, it is advantageous for Ally Online Banking to be authenticated to conduct a banking transaction using the six-digit security code.

122. On information and belief, it is advantageous for Ally to be able to determine if a transaction and/or device is properly authenticated using the security code.

123. On information and belief, the six-digit security code used to authenticate a device for Ally is unique to each customer's device.

124. On information and belief, Ally Online Banking users "[i]f you already have an Ally Bank online account with a username and password, you can log in to allybank.com from your computer. . . [and can use a] Security Code in Online Banking [which is] a 6-digit code that you can ask us to send in a text message or email when you log in from a device we don't recognize."[8]

125. On information and belief, the six-digit security code is a "The code can only be used once, and expires 20 minutes after it's sent."[9]

126. On information and belief, for Ally Online Banking users, "[i]f you're on a personal computer that you use frequently it's a good idea to register it. If you're on a friend's

[8] http://www.ally.com/help/bank/login.html
[9] *Id*.

computer or a computer used by the public you should not register it."[10]

127. On information and belief, Ally Online Banking allows users to (a) check your current Ally Bank account balance[s], (b) transfer funds between an Ally Bank Interest Checking Account, Money Market Account and Online Savings Account and non-Ally accounts, (c) see up to 18 months of account activity, (d) use Ally Email to communicate securely with Customer Care for any questions about accounts and transactions, (e) change your personal information, such as your street address, email, phone, password, secret question, and telephone Personal Identification Number (PIN), (f) search and find specific transactions, (g) use our free Bill Pay service to pay bills online, (h) place and/or remove stop payments, (i) request checks, deposit slips, and forms.[11]

128. On information and belief, for Ally Online Banking users, "[i]n Ally's online banking application you chose to have a security code sent to you via text message. This message will only be sent once for each send request."[12]

129. On information and belief, Ally "use[s] a layered security approach that includes . . . activat[ing] extra security measures like asking you a question that only you know the answer to or sending a security code to a device that you've registered. This is often called **2-step, 2-factor or multi-factor authentication**."[13]

130. On information and belief, "Many financial institutions like Ally have 2-step or 2-factor authentication built into their security solutions, but it's still smart to enable multi-factor verification on sites and devices where this feature is optional. Multi-factor authentication offers another layer of protection by asking for an extra piece of information in addition to your password, like a security code that's sent via text or a fingerprint ID. You can usually **enable 2-factor verification in your password and security settings**."[14]

---

[10] *Id*.
[11] http://www.ally.com/help/bank/login.html#regional=online-mobile-banking
[12] http://www.ally.com/messages/sms/index.html
[13] http://www.ally.com/security/
[14] https://www.ally.com/security/password-security-tips.html

131. On information and belief, Ally identifies the party associated with a transaction conducted on a device running the Ally Online Banking.

132. On information and belief, Ally receives via the Ally website information associated with a transaction request.

133. On information and belief, Ally transmits a verification request to a customer to verify a transaction.

134. On information and belief, Ally determines the authenticity of a transaction based on the six-digit security code sent from a device running Ally Online Banking.

135. On information and belief, Ally authenticates a device running Ally Online Banking using two-factor authentication.

136. On information and belief, Ally electronically determines an identification of an authorized device, such as a mobile phone or computer associated with an account, based (in part) on the six-digit security code.

137. On information and belief, the Ally website transmits data over the Internet using at least the HTTP and/or HTTPS protocols.

138. On information and belief, devices running the Ally Online Banking transmit information over a mobile network.

139. On information and belief, the six-digit security code associated with a device running Ally Online Banking can be transmitted over a mobile network.

140. On information and belief, the six-digit security code is a user ID, PIN number, password, passcode, and/or user-defined party identifier.

141. On information and belief, Ally authenticates at least one party associated with a transaction by matching the six-digit security code with data stored in one or more databases.

142. On information and belief, the authentication of a device running Ally Online Banking is determined via a second communications link. This communications link could comprise a SMS text message from or a telephone call to Ally.

143. On information and belief, the authentication of a transaction is time sensitive

such that a verification message must be received during a predetermined time period.

144. On information and belief, Ally has directly infringed and continues to infringe the ’271 patent by, among other things, making, using, offering for sale, and/or selling device verification and authentication products and/or services. Such security products and/or services include, by way of example and without limitation, use of Ally Online Banking system, which is covered by one or more claims of the ’271 patent, including but not limited to claim 19.

145. By making, using, offering for sale, and/or selling security products and/or services infringing the ’271 patent, Ally has injured St. Isidore and is liable to St. Isidore for direct infringement of the ’271 patent pursuant to 35 U.S.C. § 271(a).

146. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ’271 patent.

147. As a result of Ally’s infringement of the ’271 patent, St. Isidore has suffered monetary damages in an amount adequate to compensate for Defendants’ infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants, together with interest and costs as fixed by the Court, and St. Isidore will continue to suffer damages in the future unless Defendants’ infringing activities are enjoined by this Court.

148. Unless a permanent injunction is issued enjoining Defendants and their agents, servants, employees, representatives, affiliates, and all others acting or in active concert therewith from infringing the ’271 patent, St. Isidore will be greatly and irreparably harmed.

PRAYER FOR RELIEF

Plaintiff respectfully requests the following relief from this Court:

A. A judgment that Defendants have infringed one or more claims of the ’360 and/or ’271 patents;

B. A permanent injunction enjoining Defendants and their officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert or participation with Defendants, from infringing the ’360 and/or ’271 patents;

C. A judgment and order requiring Defendants to pay St. Isidore its damages, costs,

expenses, and prejudgment and post-judgment interest for Defendants' acts of infringement in accordance with 35 U.S.C. § 284;

D. A judgment and order requiring Defendants to provide accountings and to pay supplemental damages to St. Isidore, including, without limitation, prejudgment and post-judgment interest;

E. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to St. Isidore its reasonable attorneys' fees against Defendants; and

F. Any and all other relief to which St. Isidore may show itself to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, St. Isidore requests a trial by jury of any issues so triable by right.

Dated: September 24, 2015

Respectfully submitted,

/s/ *Marc A. Fenster*

Marc A. Fenster (CA SB No. 181067)
Brian D. Ledahl (CA SB No. 186579)
Benjamin T. Wang (CA SB No. 228712)
John K. Woo (CA SB No. 281132)
RUSS AUGUST & KABAT
12424 Wilshire Boulevard 12th Floor
Los Angeles, California 90025
Telephone: 310-826-7474
Facsimile: 310-826-6991
E-mail: mfenster@rawklaw.com
E-mail: bledahl@raklaw.com
E-mail: bwang@raklaw.com
E-mail: jwoo@raklaw.com

S. Calvin Capshaw (TX SB No. 03783900)
Elizabeth DeRieux (TX SB No. 05770585)
D. Jeffrey Rambin (TX SB SB No. 00791478)
CAPSHAW DERIEUX LLP
114 E. Commerce Ave.
Gladewater, Texas 75647

Mailing Address:
P.O. Box 3999
Longview, Texas 75606-3999
Tel. 903/236-9800
Fax 903/236-8787
Email: ccapshaw@capshawlaw.com
Email: ederieux@capshawlaw.com
Email: jrambin@capshawlaw.com

Attorneys for Plaintiff,
St. Isidore Research, LLC